REMARKS

The last Office Action in the above-identified application and the references cited by the Examiner have been carefully considered. The claims have been amended in a sincere effort to define more clearly and more specifically features of applicants' invention which distinguish over the art of record.

The allowance of Claims 1-4, 35 and 47-49 is acknowledged and gratefully appreciated. Also, Claim 7, 13, 20, 27, 33 and 34 have only been objected to as being dependent upon a rejected base claim but would be allowed once these claims are rewritten in independent form to include all of the limitations of the claims from which they depended. Accordingly, the probable allowance of these claims is also acknowledged and gratefully appreciated. Thus, Claims 7, 13, 20, 27, 33 and 34 have been amended and placed in independent form to incorporate all of the limitations of the claims from which they depended. It is respectfully urged that Claims 7, 13, 20, 27, 33 and 34 are now in proper form for allowance and such action is respectfully solicited.

Claims 5, 8-12, 14-19, 21, 23-26, 28-32 and 43-46 have been rejected as being unpatentable under 35 U.S.C. 102(e), and Claim 8 has been rejected as being unpatentable under 35 U.S.C. 103(a), in view of U.S. Patent No. 6,201,871 (Bostley et al.). With respect to independent method Claim 9 and dependent Claims 10, 11, 12 and 14, the Examiner contends that the Bostley et al. patent discloses coupling an encryption processor and an authentication process to a data bus independent of each other, as shown in Figure 3 and by reference numerals 104 and 103 of the Bostley et al. patent; performing encryption on a first data packet within the encryption processor, as shown in Figure 3 of the Bostley et al. patent; and performing authentication of the first data packet within at least one authentication processor connected to the encryption processor by the data bus, as shown in Figure 3 of the Bostley et al. patent.

With respect to independent method Claims 5 and 15, the Examiner contends that the Bostley et al. patent discloses coupling a control unit to a first data bus, in Figure 3 of the Bostley et al. patent; receiving first and second data packets in the control unit from the first data bus; coupling a plurality of processors to a second data bus independent of each other and independent of the control unit, as shown in Figure 10 and by reference numbers 103 through 105 in Figure 10; providing the plurality of processors in data communication with the control unit over the second data bus, independent of the first data bus, the processors including at least one encryption processor and at least one authentication processor, as shown in Figure 10 and disclosed at column 6, lines 11-29 of the Bostley et al. patent; providing data of the first data packet from the control unit to at least one encryption processor over the second data bus, as shown in Figures 3 and 10 of the Bostley et al. patent; the step of processing data from the first data packet with at least one encryption processor to provide output data for the first data packet from at least one encryption processor, as shown in Figure 3 of the Bostley et al. patent; communicating output data for the first data packet from at least one encryption processor to at least one authentication processor for further processing, as shown in Figure 4 of the Bostley et al. patent; and providing data from the second data packet to at least one encryption processor and processing the data from the second data packet in the at least one encryption processor while at least one authentication processor further processes the output data for the first data packet, as shown in Figure 9 of the Bostley et al. patent.

With respect to independent apparatus Claims 16 and 23 and dependent Claims 17-19, 21, 24-26 and 28, the Examiner contends that the Bostley et al. patent discloses a computer having a data storage device connected thereto, wherein the data storage device stores data, as shown in Figure 2 of the Bostley et al. patent; one or more computer programs, performed by the computer, for performing encryption on a first data packet within an encryption processor, and after completion of the encryption of the first data packet, performing authentication of the first data packet in at least one authentication processor connected to the encryption processor by a data

bus, as shown in Figures 2, 3, 6, 10 and disclosed at column 6, lines 11-29 of the Bostley et al. patent; and an encryption processor and at least one authentication processor being coupled to the local data bus independent of each other, as shown in Figure 2 of the Bostley et al. patent.

With respect to independent apparatus Claim 29, independent method Claim 30 and dependent Claim 31, the Examiner contends that the Bostley et al. patent discloses the structure and steps set forth in these claims for the same reasons which he presented with respect to independent Claim 23, mentioned previously.

Independent apparatus Claims 43 and 46 and dependent Claims 44 and 45 have also been rejected in view of the Bostley et al. patent for the same reasons the Examiner gave with respect to independent Claims 5 and 16 mentioned previously.

With respect to dependent Claim 8, the Examiner acknowledges that the Bostley et al. patent does not disclose communicating the output data over a daisy-chain connection between processes, but believes that such daisy-chain connections are well known in the art. Also, with respect to dependent Claim 32, the Examiner contends that the Bostley et al. patent discloses and shows in Figure 5 an authentication processor which performs an integrity check of output data, as claimed.

The Examiner has also rejected Claims 9 and 16 on formal grounds. He contends that it is unclear how encrypting the second data packet is performed prior to completion of authentication of the first data packet when the first data packet has been encrypted and authenticated. He states that, according to the method steps defined by Claim 9, the first packet authentication has been established before processing the second packet.

Claim 5 has been amended to more specifically point out features of applicants' invention which distinguish over the art of record. The rejection of the

remaining claims pending in the application, as well as Claim 5, in view of the Bostley et al. patent is respectfully traversed.

With respect to independent Claim 9 and dependent Claims 10, 11, 12 and 14, which depend directly or indirectly from Claim 9, the Examiner correctly points out that the Bostley et al. patent discloses an encryption processor and an independent authentication processor, and that the encryption processor performs encryption on the "first data packet". However, it is respectfully urged that the authentication processor does not perform authentication of the first data packet. In the Bostley et al. system, the authentication (in the authentication system) uses the result of the decryption to authenticate a device. This is shown in Figures 5 and 8 of the Bostley et al. patent, where there is authentication using the Shared Secret Data (SSD), but it is simply retrieved from storage. As stated at Column 5, Lines 59-62: "The device 100 and the authentication system 103 each use their internally stored SSD and a random number from the challenge message to generate AUTH." Also, the Examiner's attention is respectfully called to Column 7, Lines 5-7 of the Bostley et al. patent, where it is stated that "[b]oth the device 100 and the authentication system 103 input RANDBS, SSD, and ID INFO into CAVE to generate an SSD authentication result (AUTH)." Accordingly, it is respectfully urged that there is no involvement of the encryption device at all. None of the values used for authentication are ever sent to the secure processor.

Also, the Examiner respectfully refers to Figure 7 of the Bostley et al. patent, where it is shown that the "first packet" sent to the secure processor is for "SSD UPDATE & ENCRYPTED A-KEY". In the Bostley et al. patent, what is actually used for device authentication is the SSD retrieved from the secure processor. There is absolutely no authentication of "SSD-UPDATE & ENCRYPTED A-KEY" disclosed in the Bostley et al. patent.

The Examiner's attention is also respectfully called to Figure 9 of the Bostley et al. patent. In this figure, both the authentication is done on the secure processor,

and not on the authentication system – the authentication system merely acknowledges the result of the authentication from the secure processor. It should be further noted that in this variation of the Bostley et al. system, there is no encryption or decryption at all, as the patent clearly teaches that AUTH generation, as well as generation of the Signaling Message Encryption (SME) key or the Cellular Message Encryption Algorithm (CMEA) key, and the Voice Privacy Mask (VPM) or the CDMA Private Long Code Mask (PLCM) involve the Cellular Authentication Voice Encryption (CAVE) algorithm, which is a hash algorithm. As stated at Column 6, Line 39 of the Bostley et al. patent: "The CAVE algorithm is a known one-way hash function."

Accordingly, it is respectfully urged that Claim 9 and dependent Claims 10, 11, 12 and 14 patentably distinguish over the Bostley et al. patent for the reasons stated above and are allowable.

With respect to Claim 5 of the subject application, it is respectfully urged that there is no "control unit", as claimed in Claim 5, disclosed in the Bostley et al. patent or anything comparable to a control unit as defined by Claim 5. In Claim 5, the control unit is independent of the encryption and authentication units. However, the "authentication system" disclosed in the Bostley et al. patent, cannot be both the control unit and the authentication unit. If one were to consider the "base station" in the Bostley et al. patent as the "control unit" defined by Claim 5 of the subject application, then there are no "data packets" sent from the base station to the secure processor. In the Bostley et al. patent, data received by the secure processor is originating from the authentication system.

To address the Examiner's concerns in this regard, Claim 5 has been amended to clarify that the "encryption processor" actually encrypts or decrypts the "first data packet" – not just "processes" it.

Accordingly, for the reasons stated above, it is respectfully urged that independent Claim 5, and Claim 7 and 8, which depend directly from independent Claim 5, patentably distinguish over the references of record and are allowable.

With respect to independent Claim 16, and dependent Claims 17, 18, 19 and 21, which depend directly or indirectly from Claim 16, Claim 16 has a similar limitation to that discussed above with respect to independent Claim 9. Accordingly, it is respectfully urged that the Bostley et al. patent does not perform authentication of the first packet. Moreover, in the Bostley et al. patent, encryption is involved only for the A-Key generation, that is, encryption of A-Key value before outputting it from the secure processor. However, it is obvious that the A-Key value is generated in the secure processor, as it is never found outside the secure processor and the device. As such, the unencrypted A-Key value is never sent to the secure processor for encryption, unlike the apparatus defined by Claim 16 of the subject application.

Accordingly, it is respectfully urged that independent Claim 16 and dependent Claims 17, 18, 19 and 21, which depend directly or indirectly from independent Claim 16, patentably distinguish over the Bostley et al. patent for the reasons submitted above and with respect to the patentability of Claim 9.

With respect to independent Claim 23 and dependent Claims 24, 25, 26 and 28, which depend directly or indirectly from independent Claim 23, the article of manufacture and the method steps set forth in these claims have similar limitations to those found in method Claim 9 and apparatus Claim 16, and the arguments submitted with respect to the patentability of Claims 9 and 16 are applicable here. The Bostley et al. patent does not perform authentication of the first packet. Moreover, in the Bostley et al. patent, encryption is involved only with respect to the A-Key generation, that is, encryption of the A-Key value before outputting it from the secure processor. The A-Key value is generated in the secure processor, as it is never found outside the secure processor and the device. As such, the unencrypted A-Key value is never sent to the secure processor for encryption.

Accordingly, it is respectfully urged that independent Claim 23 and dependent Claims 24, 25, 26 and 28, which depend directly or indirectly on independent Claim 23, patentably distinguish over the Bostley et al. patent for the same reasons submitted above with respect to Claims 9 and 16.

Independent Claim 29 has limitations in defining the article of manufacture and method steps which are similar to the article of manufacture and method steps set forth in Claim 23. Accordingly, it is respectfully urged that Claim 29 patentably distinguishes over the references of record, and in particular, the Bostley et al. patent, for the same reasons submitted with respect to Claim 23 and its dependent claims. The Bostley et al. patent does not perform authentication of the first packet, and encryption in the Bostley et al. patent is involved only at the A-Key generation, that is, encryption of the A-Key value is performed before it is outputted from the secure processor, and the A-Key value is generated in the secure processor, as it is never found outside of the secure processor and the device. As such, the unencrypted A-Key is never sent to the secure processor for encryption.

Independent Claim 30 and dependent Claim 31, and the methods defined thereby, have limitations which are similar to the method defined by Claim 5 and discussed previously. In particular, there is no "control unit" disclosed in the Bostley et al. patent which functions in the same manner as that defined by Claim 30. In Claim 30, the control unit is independent from the encryption and authentication units. The "authentication system" disclosed in the Bostley et al. patent cannot be both the control and the authentication units. Even if one were to consider the "base station" in the Bostley et al. patent as the "control unit" defined by Claim 30, then there are no "data packets" sent from the base station to the secure processor in the Bostley et al. patent. In the Bostley et al. patent, data received from the secure processor is originating from the authentication system. Accordingly, the Bostley et al. patent does not teach or suggest the control unit or the functionality of the control unit set forth in Claim 30 of the subject application.

Accordingly, it is respectfully urged that independent Claim 30, and dependent Claim 31 which depends from Claim 30, patentably distinguish over the Bostley et al. patent for the reasons stated with respect to Claim 5 and further stated above, and are allowable.

Claim 32 depends from independent Claim 5 and is respectfully urged to patentably distinguish over the references of record, and in particular, the Bostley et al. patent, for the same reasons submitted with respect to independent Claim 5.

Independent Claim 43 defines a packet processor apparatus having limitations which are similar in many respects to the method defined by Claim 5 and the method defined by Claim 30. In particular, the "controller" defined thereby is not found in the Bostley et al. patent. The controller is independent from the encryption and authentication units in Claim 43. However, in the Bostley et al. patent, the "authentication system" cannot be both the controller and the authentication unit. The "base station" in the Bostley et al. patent cannot function as the "controller" defined by Claim 43, because there would be no "data packets" sent from the base station to the secure processor. In the Bostley et al. patent, data received by the secure processor is originating from the authentication system.

Accordingly, it is respectfully urged that Claim 43 and dependent Claims 44 and 45 which depend directly from Claim 43, patentably distinguish over the Bostley et al. patent for the reasons submitted above and for the reasons submitted with respect to Claim 5 and Claim 30.

Claim 46 defines a packet processor apparatus which is similar in many respects to the packet processor apparatus defined by Claim 43, discussed previously. The packet processor apparatus also includes a controller, in the same manner as the packet processor apparatus defined by Claim 43. Accordingly, it is respectfully urged that the Bostley et al. patent does not disclose a "controller", within the meaning of the term used in Claim 46 which functions in the manner set forth in Claim 46. The

same reasons as to why the packet processor apparatus defined by Claim 46 is patentable over the Bostley et al. patent were previously presented with respect to Claim 43. Accordingly, it is respectfully urged that Claim 46 patentably distinguishes over the Bostley et al. patent and is allowable.

Claim 15 defines applicants' method of processing data, which has similar steps and limitations to the method of processing data set forth in Claim 9. Claim 15 requires that encryption and authentication is performed on the first data packet. In contrast, the system and methodology disclosed in the Bostley et al. patent do not have the authentication processor perform authentication of the first data packet. As mentioned previously with respect to the patentability of Claim 9, in the Bostley et al. patent system, the authentication (in the authentication system) uses the result of the decryption to authenticate a device. This is shown in Figures 5 and 8 of the Bostley et al. patent, where there is authentication using the SSD, but it is simply retrieved from storage, as disclosed at Column 5, Lines 59-62, and at Column 7, Lines 5-7, of the Bostley et al. patent. There is no involvement of the encryption device at all. Certainly, none of the values used for authentication are ever sent to the secure processor. In Figure 7 of the Bostley et al. patent, the "first packet" sent to the secure processor is for the "SSD-UPDATE & ENCRYPTED A-KEY". What is used for the device authentication is the SSD retrieved from the secure processor. There is absolutely no authentication of the "SSD-UPDATE & ENCRYPTED A-KEY" disclosed in the Bostley et al. patent.

Also, in Figure 9 of the Bostley et al. patent, both the authentication is done on the secure processor (not on the authentication system) – the authentication system merely acknowledges the result of the authentication from the secure processor. In this particular variation of the Bostley et al. system, there is no encryption or decryption at all, as the patent clearly teaches that AUTH generation as well as generation of the SME or CMEA key and VPM or PLCM mask involve the CAVE algorithm, which is a hash algorithm, as taught at Column 6, Line 39 of the Bostley et al. patent.

Accordingly, it is respectfully urged that Claim 15 patentably distinguishes over the Bostley et al. patent for the reasons submitted above and for the same reasons submitted with respect to Claim 9.

In Paragraph 4 on Page 5 of the Office Action, the Examiner also rejected Claims 9 and 16 under 35 U.S.C. 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicants regard as the invention. With respect to Claim 9, the Examiner contends that it is unclear how encrypting the second data packet is performed prior to completion of authentication of the first data packet when the first data packet has been encrypted and authenticated. Applicants assume that a similar reasoning has been applied by the Examiner to Claim 16.

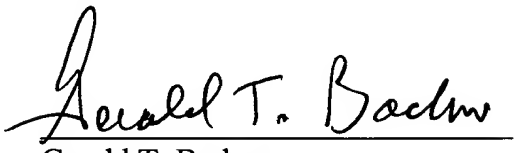
The rejection of Claims 9 and 16 under 35 U.S.C. 112 as being indefinite is respectfully traversed. With respect to the steps set forth in these claims, it is applicants' position that "performing" an operation does not mean completing the operation. In fact, if a lengthy operation is performed in a multi-processor system, other operations may start. It is clearly stated in Claims 9 and 16 that the authentication operation on the first packet and the encryption operation on the second packet are both "after completion" of the encryption of the first packet. Accordingly, it is not necessarily the case where the first packet data authentication has been completed before processing of the second packet.

If the Examiner has any further questions with respect to Claims 9 and 16 in this regard, it is respectfully requested that he contact the undersigned attorney at telephone number given below, and the undersigned attorney will be happy to discuss this issue with the Examiner.

In view of the foregoing amendments and remarks, entry of the amendments to Claim 5, 7, 13, 20, 27, 33 and 34, favorable reconsideration of Claims 5, 7-21, 23-

34 and 43-46 and allowance of the application with Claims 1-5, 7-21, 23-35 and 43-49 are respectfully solicited.

Respectfully submitted,



Gerald T. Bodner
Attorney for Applicants
Registration No. 30,449

BODNER & O'ROURKE, LLP
425 Broadhollow Road, Suite 108
Melville, NY 11747
Telephone: (631) 249-7500
Facsimile: (631) 249-4508